PCT/CN03/01160

证　　明

本证明之附件是向本局提交的下列专利申请副本

申　请　日：　2003 06 08

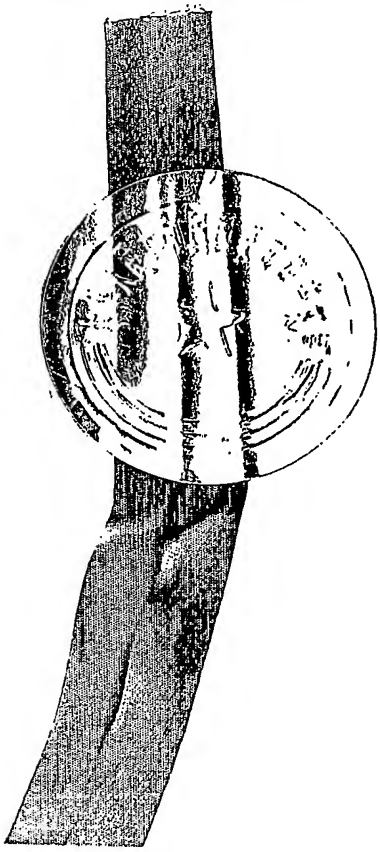
申　请　号：　03 1 37545.6

申请类别：　发明

发明创造名称：　一种虚拟私有网络的网络管理系统及其实现方法

申　请　人：　华为技术有限公司

发明人或设计人：范晓继；史扬；董欣



中华人民共和国
国家知识产权局局长　王景川

2004 年 1 月 17 日

03.06.16

权 利 要 求 书

1、一种虚拟私有网络的网络管理系统，所述网络管理系统包括供应商网络管理系统和客户网络管理系统，其特征在于：在供应商 NMS 和客户 NMS 之间设有客户网络管理代理功能模块，所述模块使用 f 接口与供应商 NMS 中的 OSF 功能模块相连，以实现客户网络管理代理。

2、根据权利要求1所述的系统，其特征在于：所述客户网络管理系统包括以下三层体系结构，即由运行于浏览器的客户层、运行于供应商网站的Web服务器中的集中控制器层和包含客户网络管理代理功能模块的事务处理层构成，客户层通过网络与集中控制器层连接，集中控制器层通过所述网络或专用线路与事务处理层连接。

3．根据权利要求2所述的系统，其特征在于：所述客户层包括浏览器和运行于浏览器上的、面向客户提供CNM的图形用户界面的CNM管理界面。

4．根据权利要求2所述的系统，其特征在于：所述集中控制器层包括运行于供应商网站的Web服务器中的请求控制器、消息编解码器和消息收发器模块。

5．根据权利要求2所述的系统，其特征在于：所述事务处理层由运行于供应商NMS中的CNM代理器构成。

6．根据权利要求2所述的系统，其特征在于：所述客户层通过客户网络设备接入所述网络，所述集中控制器层通过供应商网络设备接入所述网络；所述网络是指互联网或其它专用网。

7．一种虚拟私有网络的网络管理系统的实现方法，所述网络管理系统包括供应商NMS和客户NMS，其特征在于：所述客户NMS使用f接口与供应商NMS

的OSF模块相连进行客户网络管理代理。

8．根据权利要求7所述的方法，其特征在于：它可以包括以下步骤：

a、客户提交CNM管理功能请求；

b、将CNM管理功能请求进行解码，封装为NMS消息；

c、识别NMS消息中的CNM管理功能类型，确定所属的NMS功能模块，调用f接口将NMS消息发送给NMS相应功能模块处理；

d、将NMS相应功能模块返回的处理结果封装为NMS响应报文；

e、根据NMS响应报文生成显示页面；

f、显示页面。

9．根据权利要求8所述的方法，其特征在于：所述步骤a中在客户端浏览中完成的提交管理功能请求包括以下步骤：

a1、判断是否已经登录，如果已经登录则转到步骤a3；否则

a2、输入CNM客户信息，生成CNM管理功能请求，转到步骤a4；

a3、选择CNM的管理功能功能，生成CNM管理功能请求；

a4、发送CNM管理功能请求。

10．根据权利要求8所述的方法，其特征在于：所述步骤b实现CNM管理功能请求解码和封装成NMS消息的过程包括以下步骤：

b1、将接收到的CNM管理功能请求解码；

b2、判断请求中的数据是否完整，如果完整则转到步骤b4；否则

b3、生成错误页面，发送回客户端浏览器显示，结束；

b4、将请求封装成NMS消息。

03.06.16

说　　明　　书

一种虚拟私有网络的网络管理系统及其实现方法

技术领域

本发明涉及一种数据通信网管领域的客户网络管理（Customer Network Management，CNM）系统及其实现方法，具体说是一种基于电信管理网络（TELECOMMUNICATIONS MANAGEMENT NETWORK，TMN）功能模型的 f 接口和 WEB 技术的 CNM 代理功能（CNM Agent Function，CAF）的虚拟私有网络（Virtual Private Network，VPN）CNM 系统及其实现方法。

背景技术

利用公共网络来构建私有专用网络，称为 VPN。目前，越来越多的企业采用 VPN 搭建企业网，可以较少地关注网络的运行与维护，而由有丰富相关经验和技术储备的网络供应商承担。企业的网管系统（Network Management System，NMS）对企业网的管理，包含网络供应商提供的公共网络和私有网络的管理。其中公共网络的管理必须通过由网络供应商提供公共网络的服务接口获得必要的网络管理信息。CNM 服务可以视为网络供应商提供给企业客户的、对公共网络进行管理的手段，以便于客户的 NMS 实现监控公共网络的能力，当然这种监控只能限于与客户相关的，或者说是为客户提供服务的那一部分。VPN CNM 提供的主要服务就是网络供应商向客户展示他们的 VPN 拓扑结构、网络配置、网络状态和网络性能。

如附图1所示，在现有技术中，按照TMN功能模型，客户的NMS和网络供应商的NMS之间采用x接口对接。在现有技术中，实现CNM的方案一般是供应商

的网管系统提供对外的接口，在客户的网管系统中实现CNM的管理功能。其缺点主要是具体实施较为困难，因为使用x接口来实现两个网管系统之间的对接存在着x接口的标准化、数据安全等较多工程上的问题。

发明内容

有鉴于此，本发明提供了一种基于 TMN 功能模型的 f 接口及 WEB 技术的 CAF 的 VPN CNM 系统及其实现方法，以克服现有技术中的缺陷。

一种虚拟私有网络的网络管理系统，所述网络管理系统包括供应商网络管理系统和客户网络管理系统，其特征在于：在供应商 NMS 和客户 NMS 之间设有客户网络管理代理功能模块（CAF），所述模块使用 f 接口与供应商 NMS 中的 OSF 功能模块相连，以实现客户网络管理代理。

其中客户网络管理系统包括以下三层体系结构：即由运行于浏览器的客户层、运行于供应商网站的Web服务器中的集中控制器层和包含客户网络管理代理功能模块的事务处理层构成，客户层通过网络与集中控制器层连接，集中控制器层通过所述网络或专用线路与事务处理层连接。

所述客户层包括浏览器和运行于浏览器上的、面向客户提供CNM的图形用户界面（ Graphic User Interface, GUI）的CNM管理界面。所述集中控制器层包括运行于供应商网站的Web服务器中的请求控制器、消息编解码器和消息收发器模块。所述事务处理层由运行于供应商NMS中的CNM代理器构成。

所述客户层通过客户网络设备接入所述网络，所述集中控制器层通过供应商网络设备接入所述网络。所述网络是指互联网或其它专用网。

本发明所述的 VPN CNM 系统是对 CAF 的具体实现，其实现方法是使用 f 接口与供应商 NMS 的 OSF 模块相连进行客户网络管理代理，为客户提供 g 接

口。CAF 主要完成两大功能：（一）因为 CNM 提供的功能是 NMS 客户端功能的一个子集，因此使用 f 接口完全可以获取实现 CNM 功能所需的所有业务数据，不需要 OSF 提供新的接口；（二）使用 g 接口提供 GUI 给 VPN 业务的最终客户，采用 WEB 技术实现。本发明所述的 CAF 与 OSF 之间的 f 接口，可以采用 TMN 功能模型中的标准接口，也可根据 CAF 的功能需求进行扩充。

本发明还提供了一种虚拟私有网络的网络管理系统的实现方法，所述网络管理系统包括供应商NMS和客户NMS，其特征在于：所述客户NMS使用f接口与供应商NMS的OSF模块相连进行客户网络管理代理。

上述方法包括以下步骤：

a、客户提交CNM管理功能请求；

b、将CNM管理功能请求进行解码，封装为NMS消息；

c、识别NMS消息中的CNM管理功能类型，确定所属的NMS功能模块，调用f接口将NMS消息发送给NMS相应功能模块处理；

d、将NMS相应功能模块返回的处理结果封装为NMS响应报文；

f、根据NMS响应报文生成显示页面；

e、显示页面。

其中，步骤a中在客户端浏览中完成的提交管理功能请求包括以下步骤：

a1、判断是否已经登录，如果已经登录则转到步骤a3；否则

a2、输入CNM客户信息，生成CNM管理功能请求，转到步骤a4；

a3、选择CNM的管理功能功能，生成CNM管理功能请求；

a4、发送CNM管理功能请求。

上述步骤b实现CNM管理功能请求解码和封装成NMS消息的过程包括以下

步骤：

b1、将接收到的CNM管理功能请求解码；

b2、判断请求中的数据是否完整，如果完整则转到步骤b4；否则

b3、生成错误页面，发送回客户端浏览器显示，结束；

b4、将请求封装成NMS消息。

本发明解决了现有技术中存在的接口复杂问题。f 接口是 NMS 的 OSF 必须提供的接口，CNM 使用 f 接口完全可以获取实现其功能所需的所有业务数据，不需要 OSF 定义新的接口。同时 CAF 功能完全由供应商提供，最终客户采用 WEB 来访问 CNM 系统提供的功能，不存在工程实施中 IT 系统对接和互通的复杂接口制定问题。

本发明还解决了现有技术中的数据安全问题，CNM 计算功能完全由供应商实现，增强了供应商网管对 CNM 数据的可控制性。客户端必须通过服务器的安全认证，能够访问的数据是严格受限的。

附图说明

图 1 为现有技术的 VPN CNM 实现方案；

图 2 为本发明所述的基于 f 接口的 VPN CNM 实现方案；

图 3 为本发明所述的 VPN CNM 系统构成示意图；

图 4 为本发明所述的 VPN CNM 系统实现方法的流程图；

图 5 为本发明所述的 VPN CNM 系统实现方法管理功能请求解码和 NMS 消息封装的流程图；

图 6 为本发明所述的 VPN CNM 系统实现方法中提交管理功能请求的流程图。

具体实施方式

下面参照附图 2、3 描述本发明所述的 VPN CNM 系统。

如图 2 所示，所述 VPN CNM 系统是对 CAF 的具体实现，CAF 在使用 f 接口与供应商 OSF 模块相连，为客户提供 g 接口，CAF 的功能包括两个方面：一是使用 f 接口获取实现 CNM 功能所需的所有业务数据，不需要 OSF 提供新的接口；二是采用 WEB 技术实现 g 接口提供 GUI 给 VPN 业务的最终客户。

本发明实现 OSF、CAF 之间的接口可以使用 TMN 功能模型的标准 f 接口，也可采用在标准 f 接口基础上进行扩充实现。

如附图 3 所示，本发明所述的 VPN CNM 系统的客户网络管理系统包括以下三层体系结构，即由运行于浏览器的客户层（Client Layer）、运行于供应商网站的 Web 服务器中的集中控制器层（Controller Layer）和运行于供应商 NMS 中的事务处理层（Business Layer）构成。客户层由浏览器和运行于浏览器上的 CNM 管理界面构成，其中 CNM 管理界面向客户提供 CNM 的图形用户界面（Graphic User Interface, GUI）。集中控制器层由运行于供应商网站的 Web 服务器中的请求控制器、消息编解码器和消息收发器模块构成，负责管理业务流程的控制和通讯协议的适配。事务处理层由运行于供应商 NMS 中的 CNM 代理器（CA）构成，使用 f 接口与供应商的 NMS 连接，负责从集中控制器层收集 CNM 客户的管理请求，并委托给 NMS 各功能模块完成。客户层通过互联网或其它专用网与集中控制器层连接，客户层通过客户网络设备接入互联网或其它专用网，集中控制器层通过供应商网络设备接入互联网或其它专用网，并与事务处理层连接，连接可通过互联网实现，也可通过专用网实现，还可通过专用线路实现。

下面参照附图 4、5 描述本发明所述的 VPN CNM 系统的实现流程。利用本发明实现的 CNM 典型业务的处理流程包括 CNM 客户登录流程和 CNM 管理功能处理流程。其中，

CNM 客户登录流程如下：

1) 客户在本地浏览器端访问供应商提供的门户网站（Web 服务器），出现 CNM 系统的登录窗口；

2) 客户在登录窗口输入 CNM 客户信息（如客户名和密码）后提交认证表单；

3) 浏览器将 CNM 客户信息经 HTTP 编码后传送给 Web 服务器；

4) Web 服务器将收到的请求串转给请求控制器处理；

5) 请求控制器对请求串进行 HTTP 协议解码后，判断该请求串的数据是否完整，如完整则传送给消息编解码器处理，进入步骤 6；否则生成错误页面，发送回客户端浏览器显示；

6) 消息编解码器将解码后的参数使用 NMS 系统内部私有通讯协议重新封装成 NMS 消息，传送给消息收发器；

7) 消息收发器将 NMS 消息发送给 CA 处理；

8) CA 接收到 NMS 消息，识别出该消息是“客户登录认证消息”，并属于 NMS 系统中安全模块的业务范围，然后调用 f 接口向安全模块提出功能处理请求；

9) 安全模块收到 CA 转来的消息，立即着手处理，然后将消息处理结果回传给 CA；

10) CA 随即将消息处理结果封装成响应报文传给消息收发器；

11) 消息收发器直接将报文转给消息编解码器处理；

12) 消息编解码器将报文解码后传递给请求控制器；

13) 请求控制器根据报文封装的登录认证结果，控制客户端的 CNM 系统界面显示。如果认证成功，则直接给客户显示 CNM 系统管理功能主界面；如果认证失败，则再次显示 CNM 系统的登录界面，强制客户重新登录。

上述流程中的第 1、2、3、4、5 和 13 步骤是由 Web 浏览器、Web 服务器、请求控制器实现 TMN 功能模型的 g 接口提供给客户 GUI 的使用界面；上述流程中的第 6、7、8、9、10、11、12 步骤是由消息编解码器、消息收发器和 CA 完成使用 f 接口取得 CNM 所需数据。

CNM 管理功能处理流程如下：

1) 客户从浏览器上显示的 CNM 系统管理功能主界面上选择一具体的管理功能（如，查看客户 VPN 的拓扑）；

2) 浏览器将查看拓扑请求经 HTTP 编码后传送给 Web 服务器；

3) Web 服务器将收到的请求串转给请求控制器处理；

4) 请求控制器对请求串进行 HTTP 协议解码后，传送给消息编解码器处理；

5) 消息编解码器将解码后的参数使用 NMS 系统内部私有通讯协议重新封装成 NMS 消息，然后传送给消息收发器；

6) 消息收发器 NMS 消息发送给 CA 处理；

7) CA 接收 NMS 消息，识别出是“VPN 拓扑查询消息”，并属于 NMS 系统中的拓扑模块，然后调用 f 接口向该拓扑模块提出功能处理请求；

8) 拓扑模块收到 CA 转来的消息，立即着手处理，然后将消息处理结果回传给 CA；

9) CA 随即将消息处理结果封装成响应报文传给消息收发器；

10) 消息收发器直接将报文转给消息编解码器处理；

11) 消息编解码器将报文解码后传递给请求控制器；

12) 请求控制器根据报文中封装的客户 VPN 拓扑数据，重构拓扑图，并返回到客户的浏览器断显示输出。

上述流程中的第 1、2、3、4、5 和 12 步骤是由 Web 浏览器、Web 服务器、请求控制器实现 TMN 功能模型的 g 接口提供给客户 GUI 的使用界面；上述流程中的第 6、7、8、9、10、11 步骤是由消息编解码器、消息收发器和 CA 完成使用 f 接口取得 CNM 所需数据。

如图 6 所示，客户通过本地浏览器访问供应商提供的门户网站（Web 服务器）时有如下步骤：

（1）客户在浏览器端输入 CNM 某一管理功能请求；

（2）Web 服务器收到客户请求后，先检测一下该客户是否已经正确登录。如果客户已经登录过，那么在 Web 服务器端会有记录。

（3）若客户已登录，则显示请求的管理功能页面；若客户没有登录，则系统直接跳转到登录页面，强制客户执行登录操作。

以上所描述的仅仅是本发明的最佳实施例，而本领域的普通技术人员可以根据这里所公开的技术思想设计出不悖离本发明宗旨的其它技术方案。

说　明　书　附　图

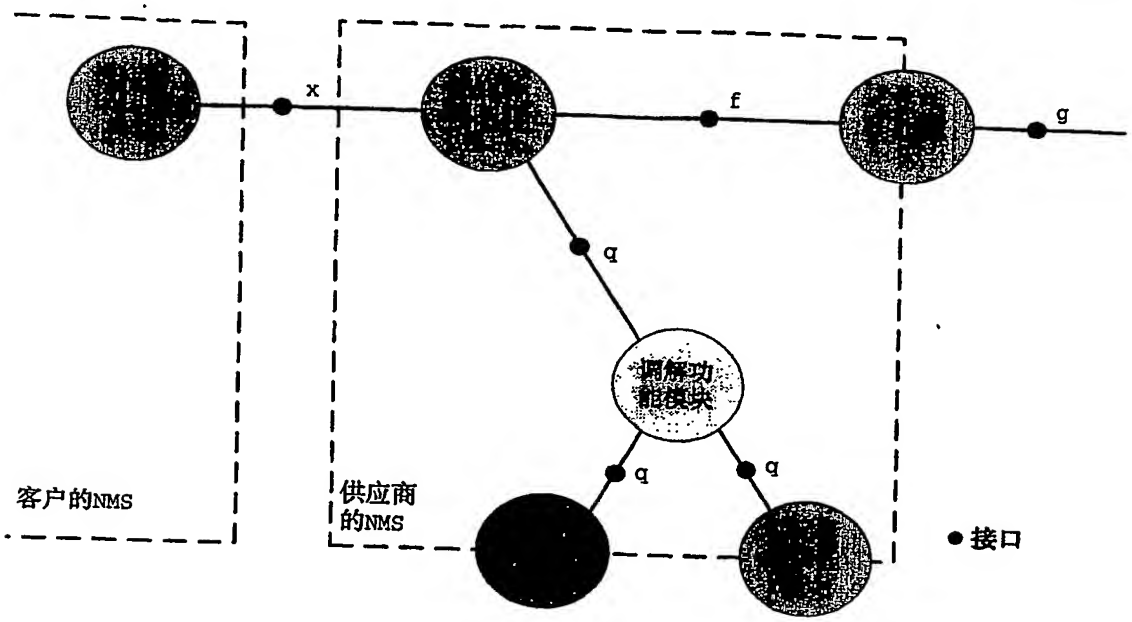

x
f
g
q
调解功能模块
q
q
客户的NMS
供应商的NMS
● 接口

图　1

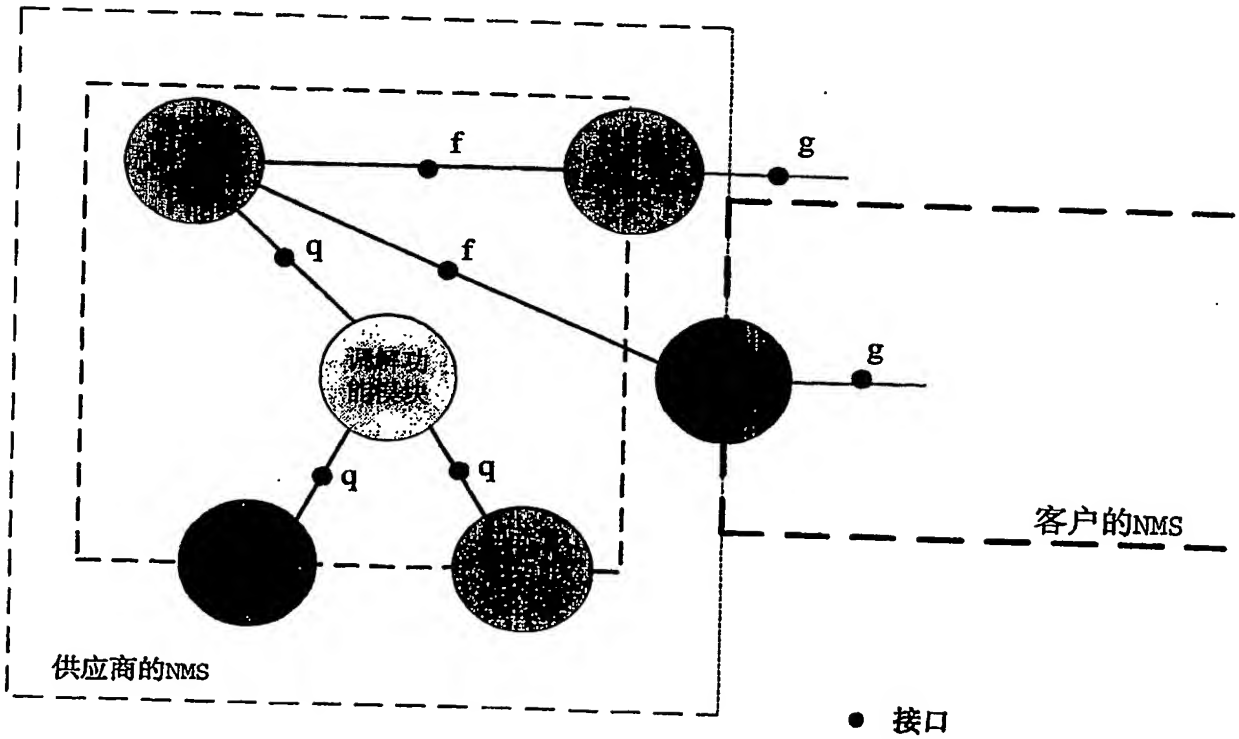

f
g
q
f
调解功能模块
g
q
q
客户的NMS
供应商的NMS
● 接口

图　2

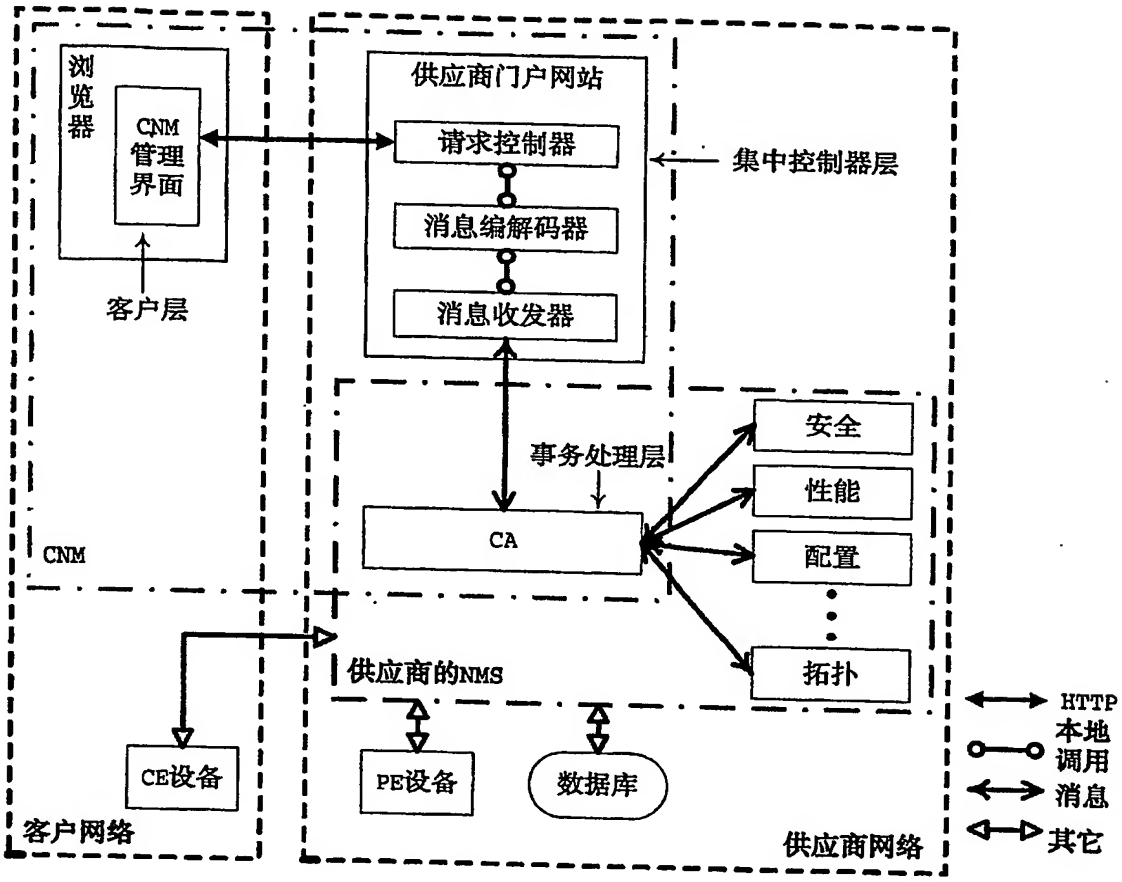

浏览器
CNM管理界面
客户层
CNM
客户网络
供应商门户网站
请求控制器
消息编解码器
消息收发器
集中控制器层
事务处理层
CA
安全
性能
配置
拓扑
供应商的NMS
CE设备
PE设备
数据库
供应商网络
HTTP
本地调用
消息
其它

图 3

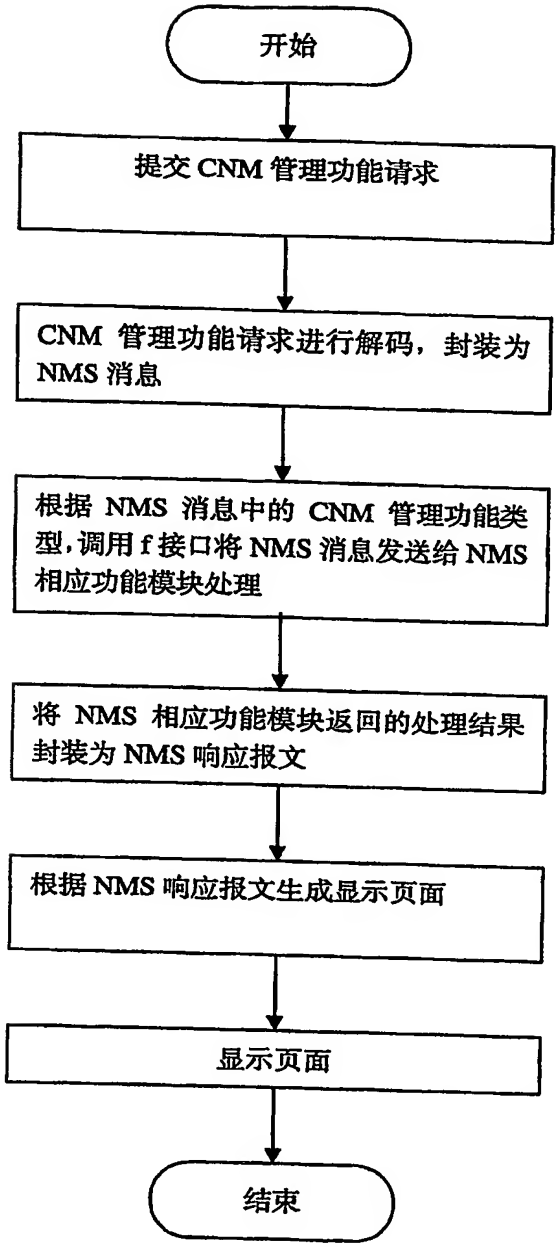

开始
提交 CNM 管理功能请求
CNM 管理功能请求进行解码，封装为 NMS 消息
根据 NMS 消息中的 CNM 管理功能类型，调用 f 接口将 NMS 消息发送给 NMS 相应功能模块处理
将 NMS 相应功能模块返回的处理结果封装为 NMS 响应报文
根据 NMS 响应报文生成显示页面
显示页面
结束

图 4

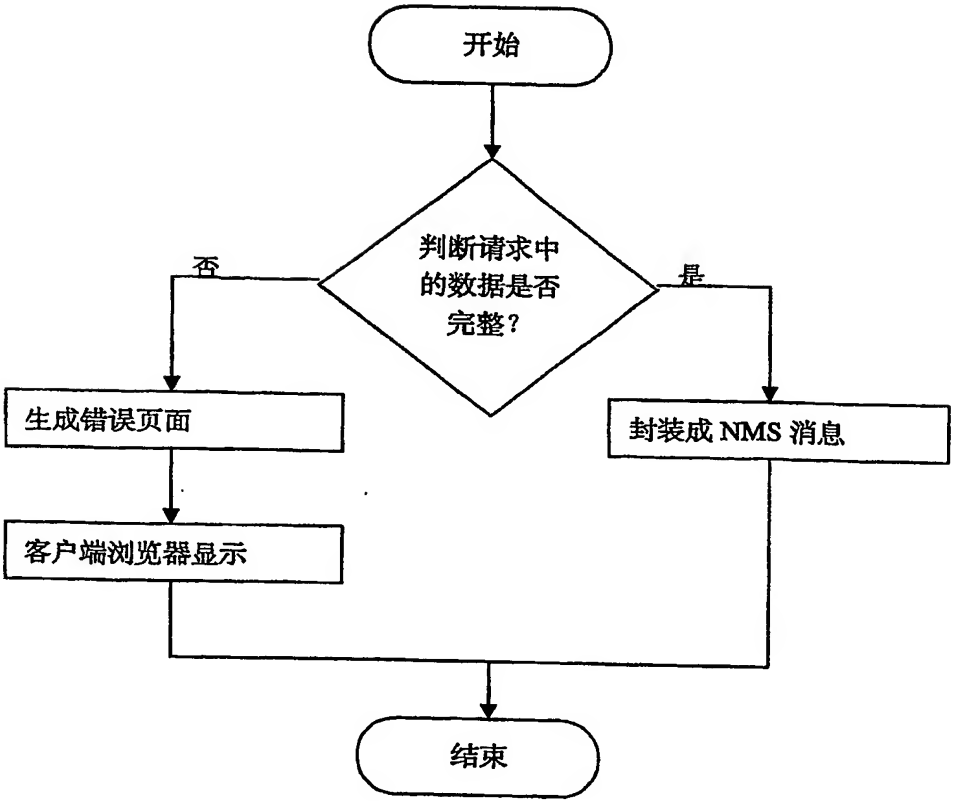

开始
判断请求中的数据是否完整?
否
是
生成错误页面
客户端浏览器显示
封装成 NMS 消息
结束

图 5

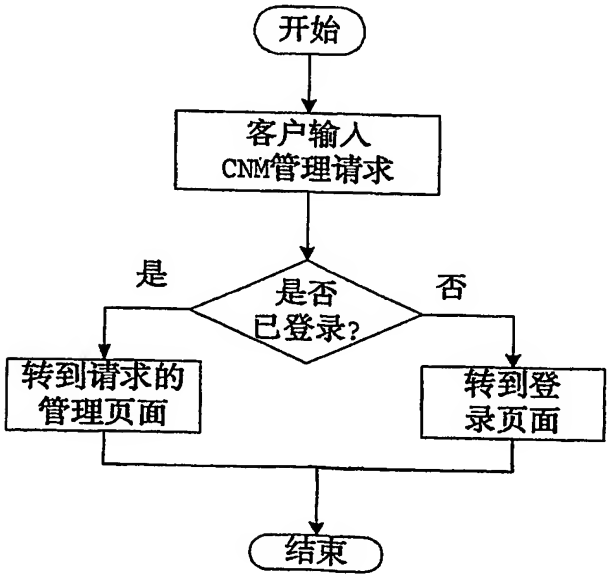

开始
客户输入CNM管理请求
是
是否已登录?
否
转到请求的管理页面
转到登录页面
结束

图 6